UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/673,658	01/04/2001	Klaus Vedder	JEK/VEDDER	3617

7590 03/29/2004

Bacon & Thomas
Fourth Floor
625 Slater Lane
Alexandria, VA 22314-1176

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	7

DATE MAILED: 03/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/673,658	VEDDER, KLAUS	
	Examiner	Art Unit	
	Andrew L Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-11 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 9 recites the limitation "the calculation." There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-3, 5-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi et al US Patent No 6,049,611 in view of Bruce Schneier "Applied Cryptography." Tatebayashi discloses a one-way data conversion apparatus and device for authentication.

6. With regards to claims 1 and 3, Tatebayashi teaches the network or network component transferring a random number to a smart card (Tatebayashi, column 6 lines 48-53), a response signal being generated from the smart card by means of an algorithm and a secret key (Tatebayashi, column 10 lines 15-22, column 9 lines 45-63), and transmitting the response signal to the network or network component (Tatebayashi, Figure 3, column 8 lines 48-54). Tatebayashi further teaches that to form the response signal the random number is split into two parts (Tatebayashi, column 7 lines 1-7 and 45-49) and one of the parts is encrypted using the secret key (Tatebayashi, column 9 lines 54-63). Tatebayashi fails to teach the splitting of the secret key into two parts for use in generating the response signal. Schneier teaches a method of splitting a key into two halves that are to be used in encrypting data (Schneier, Page 272-273, "Key Transformation"). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Schneier's method of splitting encryption keys because it offers the advantage of increasing security by using a different key with each encryption step (Schneier, Page 272-273, "Key Transformation").

7. With regards to claim 2, Tatebayashi as modified discloses that at given number of bits is selected from the encryption result and transferred as a signal response to the network (Tatebayashi, column 8 lines 48-54).

8. With regards to claim 5, Tatebayashi as modified discloses the key and random number being split into two equally long parts (Schneier, Page 272-273, "Key Transformation", Tatebayashi, column 7 lines 45-49).

9. With regards to claims 6 and 9, Tatebayashi as modified discloses that DES algorithms are used to calculate the authentication parameters (Tatebayashi, column 10 lines 46-50).

10. With regards to claim 7, Tatebayashi as modified teaches the use of the IDEA algorithm for calculating the authentication parameters (Schneier, Pages 321-323, Section 13.9). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Schneier's suggested method of encrypting using IDEA because it offers the advantage of operating at higher speeds that DES (Schneier, Pages 321-323, Section 13.9).

11. With regards to claim 8, Tatebayashi as modified teaches a compression algorithm where the output value has a smaller length than the input parameter beign used to calculate the authentication parameter (Schneier, Page 272-275, "Key Transformation" and "The S-Box Substitution"). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize a compression method because it offers the advantage of providing a nonlinear transformation that is difficult to cryptanalyze.

12. With regards to claim 10, Tatebayashi as modified discloses that a triple DES algorithm is used as an encryption algorithm (Schneier, Page 294-295, Section 12.6) whereby one first encrypts with a first part of the key, decrypts with a second part of the key, and encrypts again with the first part of the key or third part of the key (Schneier, Page 295, Figure 12.10). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Schneier's method of triple DES

because it offers the advantage of creating ciphertext that is much harder to break through a brute force attack (Schneier, Page 294-295, Section 12.6).

13. With regards to claim 11, Tatebayashi as modified discloses that the selection of the first and second part of the random number is effected in the same way in the card and the network in random or pseudorandom alternation (Tatebayashi, column 7 lines 45-49).

14. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tatebayashi et al US Patent No 6,049,611 and Bruce Schneier "Applied Cryptography." as applied to claim 1 above, and further in view of Brown et al US Patent No 5,537,474. Tatebayashi as modified fails to teach a part of the random number and one or more parts of the key being used to calculate a channel coding key. Brown teaches the random number and one or more parts of the key being used to calculate a channel coding key (Brown, column 5 lines 39-55). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Brown's method of forming a channel coding key because it offers the advantage of allowing privacy of a voice conversation (Brown, column 4 lines 60-66).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

16. Lipner et al US Patent No 5,557,346 teaches a system and method for key escrow encryption.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305 8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ALN
***

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137